REPORT TO CONGRESS

STUDY ON EMERGENCY 911 ACCESS TO WI-FI ACCESS POINTS AND SPECTRUM FOR UNLICENSED DEVICES WHEN MOBILE SERVICE IS UNAVAILABLE

Prepared by the:
Public Safety and Homeland Security Bureau

Submitted pursuant to Section 301 of the Repack Airwaves Yielding Better Access for Users of Modern Services (RAY BAUM'S) Act

March 23, 2021

I. EXECUTIVE SUMMARY

1. The Federal Communications Commission (FCC or Commission) submits this Report pursuant to Section 301 of the Repack Airwaves Yielding Better Access for Users of Modern Services (RAY BAUM'S) Act of 2018 (Section 301).[1] This Report explores the public safety benefits, technical feasibility and cost of providing the public with access to 911 services using Wi-Fi access points and other alternative means during times of emergency when mobile service is unavailable.

2. The comment record on which this Report is based points to recent improvements in the provision of voice and broadband connectivity over Wi-Fi for non-emergency communications that could be leveraged to support emergency communications as well. In the long term, these improvements could lead to Wi-Fi solutions that would expand the 911 connectivity options available to consumers, Public Safety Answering Points (PSAPs), and communications providers, and could complement the broader transition to an IP-based Next Generation 911 environment.

3. However, the comment record also indicates that today there are limits to the feasibility of providing the public with unrestricted access to 911 services over Wi-Fi or unlicensed spectrum. Existing Wi-Fi and unlicensed infrastructure typically are not engineered to provide the resiliency and reliability needed to support communications in a major emergency and are likely to be affected by many of the same conditions that impair mobile networks in such circumstances (e.g., power outages, physical damage to infrastructure from storms, floods, or wildfires). In addition, opening these platforms to the public for purposes of 911 access would require modifying or disabling authentication protocols and other safeguards, which could result in increased vulnerability.

4. Further study of the technical and policy challenges identified in this Report is required before the conditions in the evolving Wi-Fi ecosystem will support reliable provision of 911 services over Wi-Fi access points and spectrum for unlicensed devices. Commenters make clear that further work is needed to establish non-proprietary standards that would support 911 services over Wi-Fi and unlicensed spectrum. In addition, some commenters suggest that legal and regulatory changes may be needed to address liability, privacy, and security concerns with providing public access to 911 over Wi-Fi and unlicensed spectrum.

II. STATUTORY AND PROCEDURAL BACKGROUND

5. Section 301 requires that by March 23, 2021, the Commission submit to Congress and make publicly available on the Commission's website, a study on the public safety benefits and technical feasibility and cost of—

> "(1) making telecommunications service provider-owned Wi-Fi access points, and other communications technologies operating on unlicensed spectrum, available to the general public for access to 9-1-1 services, without requiring any login credentials, during times of emergency when mobile service is unavailable;
>
> (2) the provision by non-telecommunications service provider-owned Wi-Fi access points of public access to 9-1-1 services during times of emergency when mobile service is unavailable; and

[1] Repack Airwaves Yielding Better Access for Users of Modern Services (RAY BAUM'S) Act of 2018, Pub. L. 115-141, § 301, 132 Stat. 1080, 1086-87 (2018). For purposes of this study, "Wi-Fi" refers to a family of wireless network protocols, based on the IEEE 802.11 set of standards, which are commonly used for local area networking of devices and Internet access.

(3) other alternative means of providing the public with access to 9-1-1 services during times of emergency when mobile service is unavailable."[2]

6. The legislative history of Section 301 emphasizes that the study should address "making WiFi access points available to the public at no charge during times of emergency" and "focus on making WiFi access points owned by telecommunications service providers available, but should also analyze whether such a requirement would be feasible for non-telecommunications service providers."[3]

7. In June 2018, the Bureau sought comment on the effectiveness of the Wireless Network Resiliency Cooperative Framework (Framework), a voluntary initiative of the major wireless providers to develop and implement network resiliency, emergency preparation, and recovery initiatives to sustain wireless communications during and after emergencies.[4] As part of this inquiry, the Bureau noted the study required by Section 301 and sought initial comment on the feasibility of enabling 911 access to Wi-Fi access points and spectrum for unlicensed devices during emergencies.[5] The Bureau received seven comments and one reply comment addressing the Section 301 study.[6] Commenters described certain

---

[2] RAY BAUM'S Act at § 301. Section 303 of RAY BAUM'S Act defines the terms "mobile service," "WiFi access point," and "times of emergency." *Id*. § 303. Section 303(1) defines the term "mobile service" to mean "commercial mobile service (as defined in section 332 of the Communications Act of 1934 (47 U.S.C. 332)) or commercial mobile data service (as defined in section 6001 of the Middle Class Tax Relief and Job Creation Act of 2012 (47 U.S.C. 1401))[.]" *Id.* at § 303(1). Commercial mobile data service means any mobile service (as defined in 47 U.S.C. 153) that is a data service; provided for profit; and available to the public or such classes of eligible users as to be effectively available to a substantial portion of the public, as specified by regulation by the Commission. 47 U.S.C. § 1401(8). Section 303(2) of RAY BAUM'S Act defines the term "'WiFi access point'" to mean "wireless Internet access using the standard designated as 802.11 or any variant thereof." *Id*. at § 303(2). The term "times of emergency" refers to "either an emergency as defined in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122), or an emergency as declared by the governor of a State or territory of the United States." RAY BAUM'S Act at § 303(3). Section 5122 defines emergency to mean "any occasion or instance for which, in the determination of the President, Federal assistance is needed to supplement State and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States." 42 U.S.C. § 5122.

[3] Repack Airwaves Yielding Better Access for Users of Modern Services Act of 2018, H.R. Rep. No. 115-587, Title III, Sec. 301, at 30 (2018).

[4] *See* Cellular Telephone Industries Association (CTIA), "CTIA & Pallone Announce 'Wireless Network Resiliency Cooperative Framework' for Disasters and Emergencies," (April 27, 2016), https://www.ctia.org/news/ctia-pallone-announce-wireless-network-resiliency-cooperative-framework-for-disasters-and-emergencies. The Framework set out a five-pronged approach for enhancing coordination during an emergency, including providing for reasonable roaming under disaster arrangements when technically feasible. *See* Letter from Joan Marsh, AT&T; Charles McKee, Sprint; Grant Spellmeyer, U.S. Cellular; Scott Bergmann, CTIA; Steve Sharkey, T-Mobile; and William H. Johnson, Verizon, to Marlene Dortch, Secretary, Federal Communications Commission, PS Docket Nos. 11-60 and 13-239 (filed Apr. 27, 2016) (Framework), https://api.ctia.org/docs/default-source/fcc-filings/160427-final-network-resiliency-commitment-letter.pdf.

[5] *Public Safety and Homeland Security Bureau Seeks Comment on the Effectiveness of the Wireless Network Resiliency Cooperative Framework and for the Study on Public Access to 911 Services during Emergencies*, PS Docket No. 11-60, 33 FCC Rcd 5997 (PSHSB 2018) (*2018 Public Notice*).

[6] The following parties commented on the study mandated by Section 301: Association of Public Safety Communications Officials International, Inc. (APCO) Comments, PS Docket No. 11-60, at 4 (rec. Jul. 16, 2018) (suggesting that the Commission explore any "cybersecurity implications, methods of routing to the appropriate PSAP, and accurate location and callback capabilities"); National Association of State 911 Administrators (NASNA) Comments, PS Docket No. 11-60, at 2 (rec. Jul. 16, 2018) (broadly supporting making public and private Wi-Fi available without a login requirement during extreme situations); NCTA – The Internet & Television Association (NCTA) Comments, PS Docket No. 11-60 (rec. Jul. 16, 2018) (noting "a host of technical and other obstacles may limit the effectiveness of Wi-Fi hotspots for 911 access during emergencies" including an inability to

(continued….)

security risks associated with opening Wi-Fi access points for 911 service and also noted that Wi-Fi networks are reliant on power and backhaul providers to maintain operations during emergencies.[7]

8. On September 1, 2020, the Bureau issued a Public Notice seeking more detailed comment on the 911 access issues raised by Section 301.[8] Specifically, the Bureau asked commenters to "address the technical and operational complexities of giving the public access for 911 services on telecommunications service provider-owned Wi-Fi access points, including provider-owned Wi-Fi access points installed at customer premises;" the means of activating provider-owned Wi-Fi access to 911 services during "times of an emergency;" how the Wi-Fi access points would identify "911 services," including voice and data services (e.g., text-to-911); routing 911 calls to the appropriate Public Safety Answering Point (PSAP) with the caller's location information; the standards development and best practices needed to facilitate 911 services over Wi-Fi; power and backhaul capabilities that would support 911 access over Wi-Fi; and cybersecurity and privacy issues as well as congestion issues that could be associated with open access to Wi-Fi for 911 calls.[9] The Bureau received seven comments, four reply comments, and three *ex parte* comments.[10] Commenters generally supported a broader examination of

---

determine proper routing over Wi-Fi Calling and that power outages may knock out Wi-Fi capabilities; additionally recommending that regulatory action would be premature); Texas 9-1-1 Entities Comments, PS Docket No. 11-60 (rec. Jul. 16, 2018) (recommending that the Commission consider the differences of calling 911 over Wi-Fi, including identifying best practices regarding routing using a caller's physical location instead of registered location); National Emergency Number Association (NENA) Comments, PS Docket No. 11-60 (rec. Jul. 16, 2018) (recommending that "further discussion should take place with regard to 9-1-1 access over Wi-Fi, specifically in the areas of network access policies, call routing, and caller location"); AT&T Comments, PS Docket No. 11-60, at 12-15 (rec. Jul. 16, 2018) (recommending the Commission consider technical hurdles like how to disable Wi-Fi authentication, selectively prioritize traffic, and enable text-to-911 over Wi-Fi; also noting that the proposal would likely require consumer education, consideration of privacy implications, abuse prevention measures, and voluntary regulatory frameworks); T-Mobile Comments, PS Docket No. 11-60, at 9-11 (rec. Jul. 16, 2018) (recommending further study to assess the proposal's privacy, cybersecurity, and congestion implications in addition to the technical feasibility of the proposal, and recommending that the Commission refrain from taking any regulatory action to require 911 calling over Wi-Fi at this time). In reply comments, the following parties addressed the study: City of New York Reply Comments, PS Docket No. 11-60 (rec. Jul. 30, 2018) (agreeing with commenters that further study would be required before implementing 911 calling over Wi-Fi).

[7] *See, e.g.*, AT&T Comments, PS Docket No. 11-60 at 14 (rec. Jul. 16, 2018); NCTA Comments, PS Docket No. 11-60 at 5 (rec. Jul. 16, 2018)

[8] *Public Safety and Homeland Security Bureau Seeks Comment on Emergency Access to Wi-Fi Access Points and Spectrum for Unlicensed Devices Pursuant to Section 301 of RAY BAUM'S Act of 2018*, PS Docket No. 20-285, Public Notice, 35 FCC Rcd 9253 (PSHSB 2020) (*911 Wi-Fi Public Notice*).

[9] *911 Wi-Fi Public Notice*, 35 FCC Rcd at 9253-55.

[10] The following parties filed comments in response to the Bureau's *911 Wi-Fi Public Notice*: Cisco Systems, Inc., Ruckus Networks, a business segment of CommScope, and Hewlett Packard Enterprise (Joint Commenters) Comments, PS Docket No. 20-285 (rec. Oct. 1, 2020) (proposing that the scope of the report be expanded to allow 911 over Wi-Fi regardless of whether mobile network operator (MNO) networks are operational, noting that it is technically possible with caveats for enterprise Wi-Fi networks to deliver 911 calls from a mobile subscriber to a MNO, and calling for Congress to clarify that existing liability protections would apply to Wi-Fi providers); Lynk Global Inc. (Lynk) Comments, PS Docket No. 20-285 (rec. Oct. 1, 2020) (noting that their last-mile communications solution uses satellites, which could provide an alternative means of 911 access when terrestrial mobile service is unavailable); Mission Critical Partners, LLC (MCP) Comments, PS Docket No. 20-285 (rec. Oct. 1, 2020) (requesting that the Commission study further the benefits of increasing the priority of emergency calls and messages over Wi-Fi access points); NCTA Comments, PS Docket No. 20-285 (rec. Oct. 1, 2020) (urging the Commission to report to Congress that "open access to Wi-Fi APs and the delivery of 911 communications services to the public over Wi-Fi APs are not technically or operationally viable and that, while Wi-Fi hotspots can provide much-needed connectivity in some areas where CMRS radio networks are disrupted, Wi-Fi cannot substitute for MNO core networks in delivering 911 calls"); Public Knowledge (PK) Comments, PS Docket No. 20-285 (rec. Oct.

(continued….)

Wi-Fi 911 solutions, but also cited a variety of technical challenges and expressed concern about security risks and potential exposure to liability associated with opening Wi-Fi networks to unauthenticated users.

III. DISCUSSION

9. This study explores the public safety benefits, technical feasibility, and cost of options for providing the public with access to 911 services using Wi-Fi access points and other alternative means during times of emergency when mobile service is unavailable.

10. The comment record reflects that there have been recent improvements in the provision of voice and broadband connectivity over Wi-Fi for non-emergency communications that could be leveraged to support emergency communications as well. The demand for wireless broadband is growing at a phenomenal pace as the American public and businesses increasingly rely on Internet connectivity, particularly during the COVID-19 pandemic. The ubiquitous nature of Wi-Fi access points suggests that in the long term Wi-Fi based solutions could be added to the "toolbox" of 911 connectivity options available to consumers, PSAPs, and communications providers, and could complement the broader transition to an IP-based Next Generation 911 environment.[11] For example, some cable providers already allow their customers to access certain Wi-Fi hotspots,[12] and Google-Fi service allows its subscribers

---

1, 2020) (requesting that the Commission develop technical aspects of implementing emergency access over Wi-Fi, refrain from making policy recommendations until a technical framework is developed, include Wi-Fi access points that cannot transmit location data in its study, and include the ability to text 911 over Wi-Fi in this study); and Verizon Comments, PS Docket No. 20-285 (rec. Oct. 1, 2020) (urging industry collaboration to address significant technical challenges with this proposal, and requesting that the Commission account for the ubiquity of Wi-Fi access points in its report). The following parties filed reply comments: CTIA Reply Comments, PS Docket No. 20-285 (rec. Oct. 16, 2020) (asking the Commission to seek the guidance of technical expert bodies prior to submitting its report and requesting that the Commission include in its report both the limitations of mobile wireless connectivity in emergencies as well as the increasing resilience of Wi-Fi networks, even when fixed wireline backhaul and commercial power is unavailable); MCP Reply Comments, PS Docket No. 20-285 (rec. Oct. 16, 2020) (reiterating its request that the Commission study the prioritization of emergency messages over Wi-Fi access points); America's Communications Association (ACA) Reply Comments, PS Docket No. 20-285 (rec. Oct. 16, 2020) (urging the Commission to report to Congress that using Wi-Fi access points in times of emergency remains an unproven concept); NENA Reply Comments, PS Docket No. 20-285 (rec. Oct. 16, 2020) (recommending that the Commission examine whether using 911 calling over Wi-Fi would meet the expectations of the public and recommending that standards for 911 calling over Wi-Fi be established and harmonized with existing standards); and Wireless Broadband Alliance (WBA) Reply Comments, PS Docket No. (rec. Oct. 16, 2020) (suggesting that "OpenRoaming" authentication could serve as the foundation for 911 service over Wi-Fi, emphasizing the importance of field trials of 911 calling over Wi-Fi solutions, and noting that liability protections for service providers would be vital for delivering 911 service over Wi-Fi). After the close of the comment cycle, NCTA and Joint Commenters filed *ex parte* letters. *See* Letter from Danielle J. Piñeres, Vice President and Associate General Counsel, NCTA, to Marlene H. Dortch, Secretary, FCC, PS Docket No. 20-285, (rec. Nov. 27, 2020) (NCTA Nov. 27, 2020 *Ex Parte*) (requesting that the Commission report to Congress that providing 911 over Wi-Fi is not technically or operationally viable and noting the limitations of "OpenRoaming" authentication technology); Letter from Mary Brown, Senior Director, Government Affairs, Cisco Systems, Inc., Matthew MacPherson, Wireless Chief Technology Officer, Cisco Systems, Inc., Dave Wright, Head of Spectrum Policy and Standards, Ruckus Networks, a business segment of CommScope, and Chuck Lukazewski, Vice President, Wireless Strategy, Hewlett Packard Enterprise, to Marlene H. Dortch, Secretary, FCC, PS Docket No. 20-285, (rec. Feb. 8, 2021) (Joint Commenters *Ex Parte*) (reviewing Wi-Fi Calling capabilities and noting that Wi-Fi Calling would be a useful supplement to, but not a replacement for, the 911 system). *See* Letter from Danielle J. Piñeres, Vice President and Associate General Counsel, NCTA, to Marlene H. Dortch, Secretary, FCC, PS Docket No. 20-285, (rec. Feb. 23, 2020) (NCTA Feb. 23, 2021 *Ex Parte*) (discussing the call flow for a 911 call over Internet Service Provider (ISP)-provided Wi-Fi.).

[11] *See, e.g.*, Verizon Comments, PS Docket No. 20-285, at 2 (rec. Oct. 1, 2020).

[12] In 2018, the Commission noted that some multichannel video programming distributors (MVPDs) have built Wi-Fi Networks that enable subscribers to access content on mobile devices outside their homes. *See Communications*

(continued….)

using Google-Fi capable devices to seamlessly roam between T-Mobile and U.S. Cellular's networks, as well as any open and available public Wi-Fi hotspots.[13] These trends are promising and warrant further study by industry and service provider stakeholders.

11. However, commenters also raise concerns about the feasibility of providing the public with unrestricted access to 911 services over Wi-Fi or unlicensed spectrum. Absent a functioning mobile core, for example, Wi-Fi access points are incapable of connecting 911 callers to the appropriate PSAP.[14] Commenters also note that existing Wi-Fi infrastructure typically is not engineered to provide the resiliency and reliability needed to support communications in a major emergency. Even though some access points may remain functional when cell sites are down, Wi-Fi connectivity is likely to be affected by many of the same conditions that impair mobile networks in such circumstances (e.g., power outages, physical damage to infrastructure from storms, floods, or wildfires). In addition, commenters note that opening these platforms to the public for purposes of 911 access could result in increased vulnerability and exposure to liability and would require developing 911-specific authentication protocols and other safeguards.

12. Further study of the technical and policy challenges identified in this Report is required before the conditions in the evolving Wi-Fi ecosystem will support reliable provision of 911 services over unlicensed spectrum Wi-Fi access points. In particular, further work will be needed in order to establish and adopt standards to support access to 911 services over Wi-Fi and related technologies. Such standards are crucial to the development of a cohesive end-to-end system that can support the necessary interactions between mobile devices, cellular networks, Wi-Fi networks, and PSAPs when a 911 call is made. Further work is also needed to enable mobile devices to be automatically authenticated, automatically roam across telecommunication service provider and non-telecommunication service provider owned Wi-Fi access points, and be routed to the appropriate PSAP with accurate caller location information.[15] Finally, as a number of commenters point out, legal and regulatory changes may be needed to address liability, privacy, and security concerns associated with making 911 accessible to the public over Wi-Fi.

A. Technical Feasibility

1. Current Technology Limitations of Wi-Fi Calling

13. *911 Services*. Each year millions of Americans call 911 for help during emergencies—with mobile wireless service subscribers representing the great majority of calls.[16] Telecommunications

Marketplace Report, GN Docket No. 18-231, Report, 33 FCC Rcd 12558 note 146 (2018). Today, a consortium called Cable Wi-Fi, comprised of Cox, Optimum and Xfinity, has built over 500,000 hotspots typically located in high-traffic areas like businesses, hotels, restaurants and malls. *See* https://www.cablewifi.com/ (last visited Mar. 4, 2021). In addition, Xfinity Wi-Fi enables Internet consumers to connect with millions of Wi-Fi hotspots nationwide. *See* https://www.xfinity.com/learn/internet-service/wifi (last visited Mar. 4, 2021). Cox Wi-Fi allows access to over 3 million Cox Wi-Fi hotspots around the country as part of any Cox Internet plan and extends Wi-Fi access to home guests without having to provide network passwords. *See* https://www.cox.com/residential/internet/learn/cox-hotspots.html (last visited Mar. 4, 2021).

[13] *See* https://www.computerworld.com/article/3323068/google-fi-project-fi.html (last visited Mar. 5, 2021).

[14] We assume that for Wi-Fi 911 calling: 1) a 911 call is dialed by the mobile phone dialer and not by other means such as an over-the-top application; 2) the Wi-Fi access point has secure access to the mobile core; and 3) the underlying mobile core is functional.

[15] Wi-Fi calls to 911 may include voice, text (including real-time text), data, and video to accommodate varying accessibility needs.

[16] For example, in calendar year 2019, states and territories reported a cumulative total of 211,202,215 calls to 911 of all types. *See* FCC, Twelfth Annual Report to Congress on State Collection and Distribution of 911 and

(continued….)

service providers must route these 911 calls to the appropriate PSAP and provide accurate caller location with the call.[17] As technology evolves and wireline usage decreases, Congress and the Commission have taken steps to leverage new methods of providing 911 service with advanced capabilities, including indoor location information.[18] However, key technical differences remain between the delivery of a 911 call over a mobile network and delivery of the call over Wi-Fi.

14. *Wi-Fi Calling*. Wi-Fi Calling enables mobile consumers to make and receive calls over a Wi-Fi connection.[19] In 2015, wireless carriers began enabling Voice over Internet Protocol (VoIP) and Wi-Fi Calling on specific devices, where the device is connected to a Wi-Fi access point.[20] Instead of

---

Enhanced 911 Fees and Charges (Fee Report) at para. 11. https://www.fcc.gov/files/12thannual911feereport2020pdf. Of the total reported calls in 2019, states and territories reported 151,971,715 calls from wireless phones, representing approximately 72% of the total reported call volume. *Id*. The Fee Report notes that this likely understates the percentage of wireless 911 calls because some states reported total 911 calls but did not break out service categories separately. *Id*.

[17] Telecommunications carriers, including mobile wireless carriers, must "transmit all 911 calls to a PSAP, to a designated statewide default answering point, or to an appropriate local emergency authority." 47 CFR § 9.4. *See Implementation of 911 Act*, Fifth Report and Order, Memorandum Opinion and Order on Reconsideration, 16 FCC Rcd 22264, 22265, para. 1 (2001). The Commission also required wireless carriers to transmit 911 calls in accordance with former section 64.3001, now codified as 47 CFR § 9.4. *See* 47 CFR § 9.10(b). The Commission adopted this rule in 2001 in response to the Wireless Communications and Public Safety Act of 1999, which codified 911 as the national emergency number and sought to promote public safety through the deployment of a seamless, nationwide emergency communications infrastructure that included wireless communications services. Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, enacted Oct. 26, 1999, 113 Stat. 1286, amending the Communications Act of 1934, §§ 222, 251 (*Wireless 911 Act*).

[18] Section 506 of RAY BAUM'S Act reflects Congress' desire to improve 911 location accuracy across *all* technological platforms, including platforms accessible for people with disabilities. *See* Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, 132 Stat. 348, Division P, Repack Airwaves Yielding Better Access for Users of Modern Services Act of 2018 (RAY BAUM'S Act) § 506 (codified at 47 U.S.C. § 615 Notes). To implement Section 506's directive, the Commission adopted dispatchable location rules across a broad swath of technologies. Section 506 of RAY BAUM'S Act; 911 Access, Routing, and Location in Enterprise Communications Systems; Amending the Definition of Interconnected VoIP Service in Section 9.3 of the Commission's Rules, PS Docket Nos. 18-261 and 17-239, GN Docket No. 11-117, Report and Order, 34 FCC Rcd 6607 (2019), corrected by Erratum, 34 FCC Rcd 11073 (PSHSB Dec. 2, 2019). In addition, CMRS providers must deliver dispatchable location information to PSAPs when technically feasible. *Wireless E911 Location Accuracy Requirements*, PS Docket No. 07-114, Sixth Report and Order and Order on Reconsideration, 35 FCC Rcd 7752, 7775-76, para. 52 (2020) (*Sixth Report and Order*), corrected by Erratum (PSHSB Aug. 28, 2020) and Second Erratum (PSHSB Oct. 29, 2020).

[19] "Wi-Fi Calling," based on 3rd Generation Partnership Project specifications, generally refers to a service that allows mobile device to make voice calls over Wi-Fi. *See, e.g.*, 3GPP TS 24.302 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3; (Release 16) (specifying "the discovery and network selection procedures for access to 3GPP Evolved Packet Core (EPC) via non-3GPP access networks and includes Authentication and Access Authorization using Authentication, Authorization and Accounting (AAA) procedures used for the interworking of the 3GPP EPC and the non-3GPP access networks."). NENA defines Wi-Fi Calling as "[a] service offering being used by some wireless carriers, cable companies, other companies, and some enterprise customers that seek to deliver voice calls over Wi-Fi." *See, e.g.*, NENA Non-Mobile Wireless Service Interaction Information Document, at 17 (available at NENA 01-002 (ymaws.com)) (Feb. 16, 2017).

[20] *See, e.g., Transition from TTY to Real-Time Text; Petition for Rulemaking to Update Commission's Rules for Access to Support Transition from TTY to Real-Time Text, Petition for Waiver of the Rules Requiring the Support of TTY; United States Cellular Corporation*, CG Docket No. 16-145 and GN Docket No. 15-178, Order, 35 FCC Rcd 14689 para. 3 (CGB 2020). Since Section 301 of RAY BAUM'S Act focuses on using Wi-Fi access points to reach 911 when mobile service is unavailable, this study focuses on Wi-Fi Calling rather than interconnected VoIP

(continued….)

using a wireless carrier's radio access network connection, Wi-Fi Calling permits a wireless device to make a voice call or send text via a Wi-Fi access point.[21] The Wi-Fi access point service utilized by the mobile device may be supplied by a wireless carrier or by a third-party access point service provider unaffiliated with the wireless carrier, such as enterprise, or a cable provider.[22] Most newer smartphones and some tablets support Wi-Fi Calling that consumers can enable through their mobile device settings. However, older phones and feature phones may not support Wi-Fi Calling.[23]

15. *Wi-Fi 911 Call Flow*. Wi-Fi Calling uses a broadband Internet connection to make calls, including 911 calls, which causes 911 calls over Wi-Fi to be routed and transmitted differently from 911 calls made over a cellular network. First, unlike 911 calling over mobile networks, Wi-Fi Calling currently relies on the consumer to enable Wi-Fi Calling service before placing any calls, including 911 calls, over Wi-Fi.[24] Once activated for Wi-Fi Calling, the Wi-Fi access point is not capable of routing the 911 call but serves solely as a "pipe" to provide Internet access to the mobile core network, which then handles routing and further processing of the call.[25] Figure 1 illustrates, at a high-level, the Wi-Fi Calling

---

service, which are subject to 911 service requirements. The latter allows a larger range of devices, such as PCs and tablets, to make calls over the Internet. 47 CFR § 9.3 (defining Interconnected VoIP service as "An interconnected Voice over Internet Protocol (VoIP) service is a service that: (1) Enables real-time, two-way voice communications; (2) Requires a broadband connection from the user's location; (3) Requires Internet protocol-compatible customer premises equipment (CPE); and (4) Permits users generally to receive calls that originate on the public switched telephone network and to terminate calls to the public switched telephone network. Notwithstanding the foregoing, solely for purposes of compliance with the Commission's 911 obligations, an interconnected VoIP service includes a service that fulfills each of subsections (1)-(3) above and permits users generally to terminate calls to the public switched telephone network."). Unlike Wi-Fi Calling, Interconnected VoIP service is not anchored to a mobile network. Interconnected VoIP service requires a broadband Internet connection, which may be accessed through a Wi-Fi connection or another connection such as Ethernet. On the other hand, Wi-Fi Calling by definition requires a Wi-Fi connection. *Id*.

[21] The Wi-Fi connection may be a home Wi-Fi access point, or available Wi-Fi hotspot outside the home. Wi-Fi Calling is useful in areas with weak cellular coverage or with no coverage at all, so long as the device can connect to the Wi-Fi access point. If no cellular network is available, subscribers can enable Wi-Fi Calling through their device settings. https://www.verizon.com/support/wifi-calling-faqs/; https://www.att.com/features/wifi-calling/; https://www.t-mobile.com/support/coverage/wi-fi-calling-from-t-mobile.

[22] Today, most smartphones (e.g., Google Android and Apple iPhone) offered by nationwide CMRS providers (i.e., AT&T, Verizon, and T-Mobile) and Mobile Virtual Network Operators (MVNOs) such as cable companies (e.g., Charter and Comcast) and Google support Wi-Fi Calling. *See, e.g.*, Google LLC, Make calls over Wi-Fi, https://support.google.com/phoneapp/answer/2811843?hl=en (last visited Feb. 3, 2021) (describing how to set up "Wi-Fi calling"); Apple, Inc., Make a call with Wi-Fi Calling (Feb. 11, 2020), https://support.apple.com/en-us/HT203032; AT&T Inc., AT&T Wi-Fi Calling, https://www.att.com/features/wifi-calling/ (last visited Feb. 3, 2021); Verizon Wireless, Wi-Fi Calling FAQs, https://www.verizon.com/support/wifi-calling-faqs/ (lasted visited Feb. 3, 2021); T-Mobile USA, Inc., Wi-Fi Calling from T-Mobile, https://www.t-mobile.com/support/coverage/wi-fi-calling-from-t-mobile (last visited Feb. 3, 2021). Charter Communications, Spectrum Mobile, WiFi Calling FAQs, https://mobile.spectrum.com/support/article/360002088768/wifi-calling-faqs (last visited Feb. 3, 2021); Comcast, Xfinity Mobile, What is WiFi calling? (Nov. 10, 2020), https://www.xfinity.com/mobile/support/article/what-is-wifi-calling; Call emergency services (911) Google Fi Help https://support.google.com/fi/answer/6174034?hl=en (last visited Feb. 3, 2021). Joint Commenters Comments, PS Docket No. 20-285, at note 2 (rec. Oct. 1, 2020).

[23] A feature phone is a basic mobile phone that is not a smartphone. A feature phone retains the form factor of earlier generations of mobile telephones, with press-button based inputs and a small, non-touch display. *See, e.g.*, https://www.phonescoop.com/glossary/term.php?gid=131 (last visited Feb. 22, 2021).

[24] *See, e.g.*, Verizon Comments, PS Docket No. 20-285, at 4 (rec. Oct. 1, 2020).

[25] NENA Reply, PS Docket No. 20-285, at 3 (rec. Oct. 16, 2020).

architecture from mobile device (e.g., smartphone) to Wi-Fi access point to the mobile network core and ultimately to the relevant PSAP.

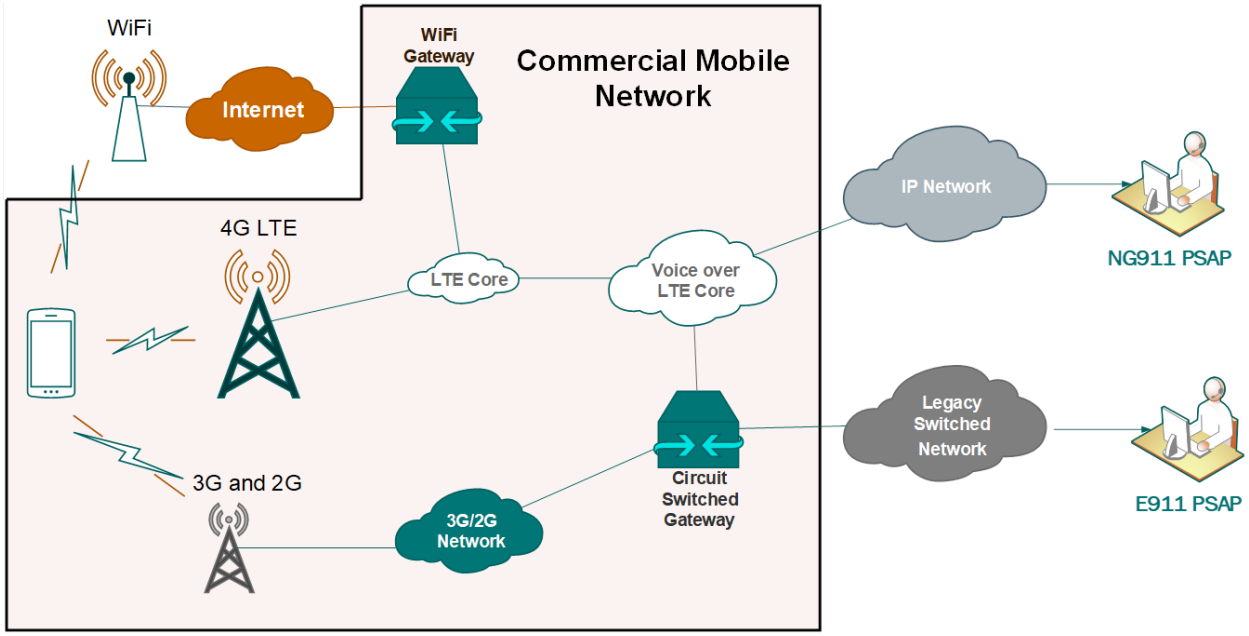


Figure 1. Wi-Fi 911 Call Flow[26]

16. *Mobile Device Interface.* The interface between the mobile device initiating the 911 call and the Wi-Fi access point represents a critical link in the Wi-Fi 911 call flow. For example, telecommunications service providers that own and manage Wi-Fi access points typically would know the locations of their access points and, under the right conditions, this information can be used in determining or refining the 911 caller location. The challenge arises when an unauthenticated mobile device attempts to connect to an unknown third-party Wi-Fi access point outside the control of the underlying CMRS provider associated with the 911 call originator. Assuming that a consumer enables Wi-Fi Calling before dialing 911 during times of emergency when mobile service is unavailable, the 911 call will face several hurdles, described below, before reaching the most appropriate PSAP.

17. *Authentication.* The principal technical hurdle to allowing Wi-Fi access points to facilitate effective and reliable 911 services during times of emergency revolves around mobile device authentication and roaming, as reflected in the Wi-Fi 911 call flow diagrams at Appendix A[27] and B.[28] The essential purpose of authentication is to provide security so that network resources such as Internet

[26] "LTE" refers to the Long-Term Evolution wireless broadband standard. In addition, "NG911" refers to Next Generation 911 and "E911" refers to Enhanced 911. For a detailed discussion on the transition from legacy 911 architecture to IP-based Next Generation 911 technology see the Report submitted pursuant to Section 6509 of the Next Generation 911 Advancement Act of 2012. Legal and Regulatory Framework for NG911 Services, Report to Congress and Recommendations (2013). https://www.fcc.gov/document/legal-and-regulatory-framework-ng911-services-report-congress.

[27] The diagram in Appendix A, provided by NCTA, highlights the following points: 1) Need to have a working mobile core and need to route the 911 call to mobile core; 2) need for caller's registered address and complications if the 911 caller has moved from the registered location; 3) need to have power and Internet connection at the Wi-Fi AP.

[28] The diagram in Appendix B, provided by the Joint Commenters, illustrates call flows for current E911 calls made over enterprise Wi-Fi networks using local or centralized authentication such as Wireless Broadband Alliance Open Roaming (WOR) or Air Pass, as well as possible enhancements that can be made to authentication and quality of service (QoS).

access can only be used by those individuals and devices that are authorized. In theory, removing these authentication requirements during times of emergency when the mobile radio access network is down would facilitate public access to 911 over Wi-Fi. However, the record reflects that such an "open Wi-Fi" approach could potentially expose networks to serious security threats such as Denial of Service (DoS) attacks on PSAPs. In discussing concerns that must be addressed before automatic authentication capabilities can be built into Wi-Fi access points, NCTA points out that "[b]roadband providers do not have control over the device or user's settings or interactions with the underlying mobile service or application provider."[29] NENA observes that "industry has developed the capability for user devices … to roam securely and without the need for manual authentication onto available Wi-Fi networks," but NENA points out that "a number of technical and business realities are necessary before the experience of connecting to 9-1-1 via a previously unknown Wi-Fi access point becomes a regular occurrence."[30]

18. *Activating Wi-Fi Access During Times of Emergency.* In addition to authentication concerns, another obstacle to making Wi-Fi access points publicly available for 911 service is that no trigger mechanism currently exists that is capable of activating Wi-Fi access points for public access in emergency-impacted areas when mobile service is unavailable and then deactivating these access points once mobile service is restored.[31] NCTA states that "[c]able broadband providers have offered voluntary no-cost Internet access during times of emergency to leverage existing Wi-Fi infrastructure for the benefit of consumers in need."[32] However, such access typically is limited to customers that have a pre-existing relationship with the service provider or have otherwise been pre-authenticated.[33]

19. *911 Call Prioritization*. Currently, Wi-Fi access points are "traffic-agnostic" and do not have the capability to distinguish emergency from non-emergency calls or to prioritize emergency calls.[34] Therefore, during times of emergency, Wi-Fi access points lack the ability to accept only 911 calls from the public and block other types of traffic such as web browsing and streaming.[35]

20. *911 Call Routing and Location.* Currently, Wi-Fi Calling does not support the automatic location functions that are needed to route 911 calls from the public to the appropriate PSAP. Most Wi-Fi access points are not location-aware, meaning that consumers enabling Wi-Fi Calling on their smartphones typically need to provide a registered address/location and manually update it as their location changes, similar to the manner in which interconnected VoIP consumers manually enter a registered address to enable 911 calling and routing.[36] If a user connects to a Wi-Fi access point and calls 911 in an area without cellular service, the mobile device will attempt to complete the call over Wi-Fi Calling and will provide the registered location.[37] If the caller is not at the registered location, the 911 call may not be routed to the closest PSAP or may be mis-routed.[38] Similarly, device-based location services that could automatically provide a caller's location (e.g., Google ELS or Apple's HELO) for a mobile 911 call may not be activated for Wi-Fi 911 Calling, and most Wi-Fi networks are not configured

[29] NCTA Comments, PS Docket No. 20-285, at 2-3 (rec. Oct. 1, 2020).

[30] NENA Reply, PS Docket No. 20-285, at 2 (rec. Oct. 16, 2020).

[31] *See, e.g.*, AT&T Comments, PS Docket No. 11-60, at 15 (rec. Jul. 16, 2018).

[32] NCTA Comments, PS Docket No. 20-285, at 4 (rec. Oct. 1, 2020).

[33] *See, e.g.*, NCTA Comments, PS Docket No. 20-285, at 4 (rec. Oct. 1, 2020).

[34] NCTA Comments, PS Docket No. 20-285, at 6 (rec. Oct. 1, 2020).

[35] *See, e.g.*, AT&T Comments, PS Docket No. 11-60 at 12 (Jul. 16, 2018).

[36] NENA Reply, PS Docket No. 20-285, at 3-4 (rec. Oct. 16, 2020).

[37] CTIA Reply, PS Docket No. 20-285, at 6 (rec. Oct. 16, 2020).

[38] NCTA Comments, PS Docket No. 20-285, at 5 (rec. Oct. 1, 2020).

either to use this information for 911 routing or to deliver the device-generated location information, such as GPS, to the appropriate PSAP.

21. *911 Callback.* A PSAP may need to call back a 911 caller in certain cases, such as when an initial 911 call is dropped. NCTA suggests that 911 calling over Wi-Fi does not typically provide the PSAP with callback capability or information. NCTA states that callbacks from PSAPs over Wi-Fi are only feasible if "a service provider that operates a Wi-Fi [access point] serves as the 'last mile' connection" and if "the [mobile network operator] core network routes the call."[39]

22. *Text-to-911.* Wi-Fi access points typically are not configured to support text-to-911. This limitation is reflected in the Commission's text-to-911 rules, which apply to CMRS providers and covered text providers but exempt text messages sent from Wi-Fi when a CMRS network is not otherwise available.[40]

23. *Power and Backhaul.* Wi-Fi networks and mobile wireless networks both depend on the availability of electrical power and backhaul connectivity to provide service in areas affected by emergencies.[41] Thus, in areas where mobile networks are not available due to power outages and/or backhaul failures, service over Wi-Fi or other communications technologies operating on unlicensed spectrum may also be unavailable, limiting their viability as emergency backup platforms for 911. And while an individual Wi-Fi access point may be able to operate on a generator and without access to backhaul, NCTA submits that "it would only be able to provide local connections to its client devices. It would not be able to connect those devices to distant locations, such as an MNO [mobile network operator] network, the Internet backbone, or a PSAP."[42]

24. *Non-Telecommunications Service Providers.* Cisco Systems, Ruckus Networks, and Hewlett Packard Enterprise (the Joint Commenters) note that a significant percentage of the nation's Wi-Fi infrastructure consists of premises-based Wi-Fi networks operated by public and private enterprises.[43] The Joint Commenters state that "advances in technology make it technically possible – *with caveats* . . . – for enterprise Wi-Fi networks to deliver 911 calls from a subscriber mobile device to their voice service provider, typically a MNO."[44] Joint Commenters state that "[s]ome of the caveats require the MNOs to adjust how their affiliated user devices operate in order to enable a user to immediately access an available Wi-Fi network. In addition, there are some challenges in the ability to deliver an accurate dispatchable address, particularly if the user is physically adjacent to an enterprise location, but within range of an enterprise Wi-Fi network."[45]

2. Technical Improvements to Wi-Fi Calling Needed to Support 911

25. *Automatic Log-On to Wi-Fi Access Points.* The Joint Commenters state that in the 2000s, industry recognized that "the need to log on separately to each Wi-Fi network every time a user wanted to

---

[39] NCTA Comments, PS Docket No. 20-285, at 10 (rec. Oct. 1, 2020).

[40] *Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Applications; Framework for Next Generation 911 Deployment, Report and Order and Further Notice of Proposed Rulemaking*, PS Docket Nos. 10-255 and 11-153, 29 FCC Rcd 9846, 9898-99, paras. 125-126 (2014).

[41] *See, e.g.*, CTIA Reply, PS Docket No. 20-285, at 3-4; (rec. Oct. 16, 2020); NCTA Comments, PS Docket No. 20-285, at 3, 12-13 (rec. Oct. 1, 2020).

[42] NCTA Comments, PS Docket No. 20-285, at 12 (rec. Oct. 1, 2020).

[43] Joint Commenters Comments, PS Docket No. 20-285, at 1 (rec. Oct. 1, 2020). Appendix B in this Report reflects the Wi-Fi 911 call flow over enterprise networks today and with potential enhancements. *See* Joint Commenters Feb. 11, 2021 *Ex Parte* at Attachment.

[44] Joint Commenters Comments, PS Docket No. 20-285, at 3 (emphasis in original) (rec. Oct. 1, 2020).

[45] Joint Commenters Comments, PS Docket No. 20-285, at 3 (emphasis in original) (rec. Oct. 1, 2020).

access the network was onerous and a barrier to achieving the full value of Wi-Fi."[46] Consequently, industry has developed mechanisms that expand the availability of automated network access to Wi-Fi networks, although these mechanisms are not configured to support unrestricted public access.

26. One such mechanism cited by the Joint Commenters is Passpoint, an "industry-wide solution that streamlines Wi-Fi access and eliminates the need for users to find and authenticate a network each time they visit."[47] The Joint Commenters state that Passpoint "was based on IEEE 802.11u" (2011), which included signaling flags "to indicate that the Wi-Fi network supports emergency services."[48] However, as NCTA notes, Passpoint only benefits consumers "that have selected a particular network provider and affirmatively connected their device or devices to that network."[49] NCTA states that "a person who is not a subscriber of the services provided by the Wi-Fi network operator cannot automatically connect and authenticate with a Wi-Fi [access point] . . . ."[50]

27. The Joint Commenters also cite the recent introduction of three commercial roaming exchange services introduced in 2020 to facilitate automatic authentication of Passpoint-capable devices:

> 1) OpenRoaming, which "makes it easy for any party operating a Wi-Fi network to allow roaming in a way that assures the security of the host network, the security of the messages to and from the roaming device while on a host network, and that allows the host network operator to define how it will participate;"[51]
>
> 2) Air Pass, which has a centralized architecture "with a curated set of participating IDPs;"[52] and
>
> 3) Orion Wi-Fi, which "employs its own solution for interconnecting venues with identity providers."[53]

28. Of the three commercial roaming exchange services, commenters focused mainly on OpenRoaming. WBA notes that "[m]ultiple commenters document that automatic discovery of and attachment to Wi-Fi networks is both feasible and an area of rapid market innovation."[54] WBA states that "[t]echnical advances in Wi-Fi networks – including but not limited to WBA OpenRoaming – provide the building blocks to augment the 911 system with Wi-Fi in certain circumstances.[55] Nevertheless, WBA

---

[46] Joint Commenters Comments, PS Docket No. 20-285, at 4 (rec. Oct. 1, 2020).

[47] Joint Commenters Comments, PS Docket No. 20-285, at 5 (rec. Oct. 1, 2020); https://wi-fi.org/discover-wi-fi/passpoint (last visited Jan. 14, 2021).

[48] Joint Commenters Comments, PS Docket No. 20-285, at 5 (rec. Oct. 1, 2020).

[49] NCTA Comments, PS Docket No. 20-285, at 7 (rec. Oct. 1, 2020).

[50] NCTA Comments, PS Docket No. 20-285, at 7-8 (rec. Oct. 1, 2020).

[51] Joint Commenters Comments, PS Docket No. 20-285, at 6 (rec. Oct. 1, 2020) citing https://wballiance.com/wba-assumes-control-of-openroaming/. The Joint Commenters raise a caveat: "the 802.11u emergency services flags in the Internetworking element have not been implemented and are not currently supported by OpenRoaming." Joint Comments, PS Docket No. 20-285 at 7 (rec. Oct. 1, 2020).

[52] Joint Commenters Comments, PS Docket No. 20-285, at 7 (rec. Oct. 1, 2020) citing https://blogs.arubanetworks.com/spectrum/aruba-air-pass-the-bridge-from-wi-fi-6-to-5g/. The service "automatically and securely authenticate[s] guests with public cellular network credentials on private enterprise Wi-Fi networks." *Id*.

[53] Joint Commenters Comments, PS Docket No. 20-285, at 7 (rec. Oct. 1, 2020) citing https://blog.google/technology/area-120/orion-wifi/.

[54] WBA Reply, PS Docket No. 20-285, at 3 (rec. Oct. 16, 2020) (later citing Joint Commenters Comments, PS Docket No. 20-285, at 5 (rec. Oct. 1, 2020), Verizon Comments, PS Docket No. 20-285 at 2 (rec. Oct. 1, 2020), PK Comments, PS Docket No. 20-285 at 1 (rec. Oct. 1, 2020).

[55] WBA Reply, PS Docket No. 20-285, at 8 (rec. Oct. 16, 2020).

"agree[s] with NCTA, Public Knowledge and other commenters that there is significant work to be done before Wi-Fi and OpenRoaming are ready to be relied upon as part of the nation's 911 infrastructure."[56] WBA notes that OpenRoaming currently supports a wide range of authentication credentials, and could support emergency services access for a wide array of Wi-Fi connected users and devices.[57] But WBA states that "it would be necessary for each of the major domestic MNOs to enable automatic SIM authentication over OpenRoaming."[58]

29. NCTA echoes this sentiment, stating that "some pre-established relationship between the guest devices and the Wi-Fi network must be established, for example between the mobile network operator (MNO) of the subscriber device and the OpenRoaming federation."[59] NCTA states that "authentication technologies such as OpenRoaming . . . cannot actually enable the provision of 911 services over Wi-Fi. Automatic authentication of a Wi-Fi device to a Wi-Fi network in the case of emergency is only one small piece of a vast and complicated puzzle . . . ."[60]

30. *Mobile Core Access and Authentication.* In addition to providing for automatic log-on to Wi-Fi access point, 911 calling over Wi-Fi requires further authentication when the call reaches the mobile network core. Since traffic could be coming from either an access point that is already recognized in the network (a so-called "trusted" access point, such as one managed by the mobile provider) or an unrecognized access point (an "untrusted access point, such as one managed by an unaffiliated third party), 3GPP provides two potential solutions: Attachment through Trusted Wi-Fi Access Gateway (TWAG) for trusted access points or an enhanced Packet Data Gateway (ePDG) for untrusted access points. For an illustration of how 3GPP handles mobile core network access and authentication," see the diagram in Appendix C.[61]

31. *Limiting Access to 911 Services Only*. While the expansion of automatic access to Wi-Fi networks could be further leveraged to support access to 911 in emergencies, the record reflects that no technical solution yet exists to limit such service to 911 calling only. Without such a limitation, allowing the public to access Wi-Fi networks without authentication or logon credentials would open such networks to all traffic, not just 911 calls. To limit access to 911 calling only, Verizon states that Wi-Fi access points will need to be able to identify "911 services" via a provisioning system tied to a smartphone, with an application that notifies the access point to enable a containerized router service, whereby a program such as a "911 Wi-Fi service on demand" is installed and activated as needed on service provider- or customer-owned equipment.[62] Verizon advises that "[i]ndustry should implement this capability using non-proprietary standards to minimize costs to—and maximize availability for—

[56] WBA Reply, PS Docket No. 20-285, at 6 (rec. Oct. 16, 2020).

[57] WBA Reply, PS Docket No. 20-285, at 5 (rec. Oct. 16, 2020).

[58] WBA Reply, PS Docket No. 20-285, at 6 (rec. Oct. 16, 2020) (noting that "at this time the 802.11u emergency services flags in the Internetworking element have not been implemented and are not currently supported by OpenRoaming. If OpenRoaming were to be used to facilitate emergency calling, it is advisable to add this capability.").

[59] NCTA *Ex Parte*, PS Docket No. 20-285, at 2-3 (Nov. 27, 2020) (noting that "OpenRoaming represents merely one authentication framework, and any potential recommendation should adhere to the Commission's longstanding commitment to technology neutrality without elevating or mandating a single technological standard.").

[60] NCTA *Ex Parte*, PS Docket No. 20-285, at 3 (Nov. 27, 2020).

[61] 3GPP provides standard-based network architecture and call flow for calls coming from both trusted and untrusted Wi-Fi networks to the mobile core, and uses an Authentication, Authorization and Accounting (AAA) server to specify how the device can be authenticated by the mobile network and which services the user is authorized to access.

[62] Verizon Comments, PS Docket No. 20-285, at 2-3 (rec. Oct. 1, 2020).

broadband and other providers, manufacturers, and public safety stakeholders."[63] Verizon recommends that standards bodies consider a wide range of technical issues, including whether 911 availability is established dynamically without input from the Wi-Fi system owner or operator, or statically with input from the owner or operator and how to ensure the 911 call is routed to the appropriate PSAP with accurate calling party/callback number and location information.[64] Verizon further advises that "[a]ddressing these issues will require substantial time, investment, and engagement by device and network equipment manufacturers, standards bodies, wireless companies and public safety stakeholders."[65] Verizon recommends that the Commission encourage the parties to begin these efforts.[66]

32. *Service Set Identifier (SSID)*. Another approach to expanding Wi-Fi access for 911 purposes would be to have all routers partitioned with an external facing SSID. As a general matter, SSIDs function to connect mobile devices to Wi-Fi access points. AT&T notes that Wi-Fi access points "can be configured into multiple logical networks (or SSIDs), and each SSID, separately, can be made open to the general public (such as in coffee shops and restaurants), or limited to a private class of users who have an expectation that their data and devices remain secure from the public internet."[67] AT&T also advises that if SSIDs are used to open up Wi-Fi access points to the general public, "this policy should be limited in application to just the public SSIDs and in no way be applied to private SSIDs."[68]

33. *Guest Networks*. A third approach to expanding 911 access over Wi-Fi in emergency-impacted areas would be to remotely link centrally managed Wi-Fi access points and create an ad hoc "guest" network. In discussing a voluntary roaming framework for enterprises, the Joint Commenters observe that "industry has developed the capability for user devices (also known as client devices) to roam securely and without the need for manual authentication onto available Wi-Fi networks, and the broad utilization of enterprise guest networks means that most enterprises could easily be able to participate."[69] From a technical standpoint, the firewall of the guest network could be configured to only accept 911 calls and provide that connection with the highest QoS. Alternatively, Wi-Fi access points on the guest network could an allow access to guest users mobile core will decide which services can be accessed and completed. That is the mobile network will reject (*not authorize*) any service request other than for a 911 call. Mobile devices could be authenticated by the central authentication solution using their mobile (SIM) credentials. This option would depend on several factors, including an agreed upon centralized authentication solution, the rate of adoption of that solution, as well as addressing privacy and liability concerns.

34. *Session Initiated Protocol (SIP) Invite*. SIP is a protocol that enables real time communications over the Internet, and Wi-Fi 911 calls typically will be SIP calls, as reflected in Appendix B. The SIP format allows location information to be inserted in the "SIP INVITE" header segment that initiates the 911 call.[70] Thus, if Wi-Fi Calling is configured to obtain location information

---

[63] Verizon Comments, PS Docket No. 20-285, at 3-4 (rec. Oct. 1, 2020) (stating that technical standards potentially implicated by such an effort include those used for Wi-Fi 6 GHz service running on dedicated channels, and mobility network 3GPP extended protocols).

[64] Verizon Comments, PS Docket No. 20-285, at 3 (rec. Oct. 1, 2020).

[65] Verizon Comments, PS Docket No. 20-285, at 3 (rec. Oct. 1, 2020).

[66] Verizon Comments, PS Docket No. 20-285, at 3 (rec. Oct. 1, 2020).

[67] AT&T Comments, PS Docket No. 11-60, at 14 (rec. Jul. 16, 2018).

[68] AT&T Comments, PS Docket No. 11-60, at 14 (rec. Jul. 16, 2018).

[69] Joint Commenters, PS Docket No. 20-285, at 3 (rec. Oct. 1, 2020).

[70] For example, AT&T advises consumers that "If you can't be located using location information obtained from your device, we'll route 911 calls based on the address you provide in your device's Wi-Fi Calling settings." *See* https://www.att.com/support/article/wireless/KM1063258/.

automatically from the user's device and insert it in the SIP header, the mobile network switch could use the information to route the 911 call to the appropriate PSAP.

B. Policy Issues

35. *Industry Coordination.* The record reflects that the complex and competitive nature of today's communications ecosystem impacts 911 service over Wi-Fi access points and spectrum for unlicensed devices.[71] NCTA states that "[f]or call hand-off to work on all Wi-Fi [access points] in emergency situations would require even more complex coordination. All providers likely would need to agree to support every transmission and compression protocol, or all providers would need to agree on one standard."[72] NCTA observes that "[t]his also presents competitive concerns, as each time an [Original Equipment Manufacturer] or service provider develops a new technology it would potentially have to share that technology with all providers."[73]

36. Verizon observes that "some providers of public Wi-Fi access networks and systems already market the coverage of their systems and their voice over Wi-Fi capabilities in the competitive marketplace in a manner similar to licensed wireless providers."[74] However, Verizon submits that the broader industry to date has not widely embraced the use of Wi-Fi access points for direct 911 call routing or as a means of delivering dispatchable location information to PSAPs.[75] Verizon concludes that "[u]sing Wi-Fi access points for 911 services as Congress contemplated in RAY BAUM'S Act will thus require a reassessment of the Commission's traditional approach to 911 regulation."[76]

---

[71] *See, e.g.*, Verizon Comments, PS Docket No. 20-285, at 4 (rec. Oct. 1, 2020). As noted in the 2020 Communications Marketplace Report, cable providers have entered the mobile wireless market through MVNO arrangements, and offer "products that rely on combining the mobile networks of facilities-based partners with hotspot or small-cell networks that send traffic through the cable provider's infrastructure." *See 2020 Report* at 6-7, para. 13. In addition, in 2015, Google launched "Project Fi" (now Google Fi), "an MVNO in partnership with T-Mobile and Sprint whereby Google Fi subscribers switched between Wi-Fi networks and these two service providers' 4G LTE networks." *See 2020 Report* at 6, para. 12.

[72] NCTA Comments, PS Docket No. 20-285, at 11 (rec. Oct. 1, 2020).

[73] NCTA Comments, PS Docket No. 20-285, at 11, n. 10 (rec. Oct. 1, 2020).

[74] Verizon Comments, PS Docket No. 20-285, at 5 (rec. Oct. 1, 2020). In addition, databases of Wi-Fi access point information are increasingly important in supporting location-based services, including for wireless E911 location accuracy. *Id.* In the Commission's *Wireless E911 Location Accuracy* proceeding, the Commission explored issues associated with Wi-Fi communications and indoor location accuracy. *See Wireless E911 Location Accuracy Requirements*, Fourth Report and Order, 30 FCC Rcd 1259 (2015) (*Indoor Location Fourth Report and Order*). The record in that proceeding demonstrated that conflicting concerns contributed to the significant challenges with leveraging Wi-Fi access points for improved indoor location accuracy. *See, e.g.*, Verizon Comments, PS Docket 07-114, at 2 (rec. Feb. 21, 2020) ("Third party providers of those services and products all have their own business and policy priorities that may not always coincide with one another, or with service providers' E911 compliance demands. And these challenges have become far more acute in recent years, as reflected in the record of this proceeding."); NCTA Reply, PS Docket 07-114, at 10-13 (rec. Jun. 18, 2019) (stating that "customer Wi-Fi access point data is commercially sensitive information, and NCTA's members are troubled by the potential for disclosure or other misuse of their customers' Wi-Fi access point information for competitive purposes.").

[75] Verizon Comments, PS Docket No. 20-285, at 5-6 (rec. Oct. 1, 2020). Verizon submits that "Any comprehensive assessment of this issue must thus also involve handset and consumer device manufacturers, in addition to manufacturers of Wi-Fi equipment and operators of public systems. While the Commission has previously applied 911 call processing requirements to analog handsets, it has almost exclusively leaned on service providers to bring new 911 capabilities to fruition. Wireless companies can support equipment manufacturers' and operators' efforts to develop and test these capabilities, but Wi-Fi-based services operate using unlicensed spectrum under the Commission's Part 15 rules." Verizon Comments, PS Docket No. 20-285, at 5-6 (rec. Oct. 1, 2020).

[76] Verizon Comments, PS Docket No. 20-285, at 6 (rec. Oct. 1, 2020).

37. *Privacy, Security and Consumer Education*. Commenters suggest that privacy and security concerns could limit the availability of reliable 911 services over Wi-Fi access points.[77] Section 551 of the Communications Act prohibits cable operators from collecting personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber.[78] NCTA states that "both Section 631 of the Communications Act and the Federal Trade Commission's privacy regime could limit a cable Wi-Fi network operator's ability to provide personal identifying information (PII), such as an address or device identifying information associated with a Wi-Fi AP or client device, to a PSAP."[79]

38. Regarding security, some commenters observe that automatically authenticating unknown end-user devices to Wi-Fi access points presents cybersecurity concerns, such as making handsets and networks susceptible to deceptive or fake access points deployed by bad actors to congest networks during times of emergency.[80] NCTA states that "[s]imply deactivating the normal authentication processes in order to facilitate open access to Wi-Fi [access points] to all comers would undermine network security."[81] AT&T observes that opening public Wi-Fi access points may expose customers and their devices to external threats during disasters when customers are most vulnerable.[82] AT&T adds that "[b]ad actors could seize upon an opportunity to spoof Wi-Fi connections during a crisis if Wi-Fi access points are open and susceptible. The Commission will need to consider options for minimizing these risks."[83]

39. AT&T emphasizes that implementing an open Wi-Fi proposal will require substantial consumer education efforts.[84] AT&T notes that consumers are conditioned not to trust unauthenticated, or unlocked, Wi-Fi and are often warned that public Wi-Fi may not be secure and are advised not to permit

---

[77] *See, e.g.*, NCTA Comments, PS Docket 20-285, at 17-18 (rec. Oct. 1, 2020) ("Enabling widespread public access to 911 services over Wi-Fi in emergencies absent a functional CMRS network presents significant privacy and security concerns"); Public Knowledge Comments, PS Docket No. 20-285, at 5 (rec. Oct. 1, 2020) ("if the FCC does not carefully consider how the technology of allowing emergency access to Wi-Fi works, it may end up harming the public by weakening network privacy and security protections. If allowing the public to access 911 over certain Wi-Fi connections creates opportunities for bad actors to breach consumer data, the public harm might outweigh the public benefits.").

[78] 47 U.S.C. § 551(b). Cable operators may collect this information, if necessary, to render cable television or other service to the subscriber or to detect unauthorized reception of cable communications. 47 U.S.C. § 551(b)(2). In addition, cable operators generally are also prohibited from disclosing personally identifiable information without the prior written or electronic consent of the subscriber. 47 U.S.C. § 551(c)(1). Section 551 states that "a cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator." 47 U.S.C. § 551(c)(1). "Other service" is defined as "any wire or radio communications service provided using any of the facilities of a cable operator that are used in the provision of cable service." 47 U.S.C. § 551(a)(2)(B).

[79] NCTA Comments, PS Docket No. 20-285, at 17 (rec. Oct. 1, 2020).

[80] *See, e.g.*, T-Mobile Comments, PS Docket 11-60, at 10 (rec. Jul. 16, 2018); Verizon Comments, PS Docket No. 20-285, at 2 (rec. Oct. 1, 2020); MCP Comments, PS Docket No. 20-285, at 18 (rec. Oct. 1, 2020).

[81] NCTA Comments, PS Docket No. 20-285, at 17-18 (rec. Oct. 1, 2020) (states that "[a]s a result, new automatic authentication protocols would need to be developed with adequate security built in at the outset and be widely adopted and implemented across the Wi-Fi and end-user device ecosystem.").

[82] AT&T Comments, PS Docket No. 11-60, at 14 (rec. Jul. 16, 2018).

[83] AT&T Comments, PS Docket No. 11-60, at 14 (rec. Jul. 16, 2018) (footnote omitted).

[84] AT&T Comments, PS Docket No. 11-60, at 13 (rec. Jul. 16, 2018).

their devices to auto-connect to public Wi-Fi networks that are not password protected.[85] AT&T points out that by default, most devices do not automatically register on Wi-Fi when operating in the vicinity of an unauthenticated Wi-Fi network, and to avoid confusion during an emergency, consumers will need to be educated about the availability and appropriate use of open Wi-Fi access points during emergencies.[86]

40. *Liability*. Some commenters urge Congress to explicitly extend liability protection applicable to wireless and VoIP service providers to operators of Wi-Fi access points in providing emergency communications and releasing subscriber information.[87] NCTA contends "Congress would need to make clear that a Wi-Fi network operator is providing an 'emergency communications service' and 'releas[ing] . . . information' to a PSAP or otherwise provide equivalent protection before encouraging or requiring access to Wi-Fi APs for 911 services without a functional underlying CMRS network."[88] In addition, NCTA observes that "Net 911 Act's protections are limited because those protections depend on the protections afforded to [Local Exchange Carriers] under individual state laws. State laws, in turn, can impose meaningful limitations on this immunity."[89] The Joint Commenters echo NCTA's request that Congress revisit liability protection and state that enterprises and Wi-Fi vendors may be reluctant to support 911 over Wi-Fi if they "risk incurring liability for uncompleted, dropped or misrouted 911 calls . . ."[90] The Joint Commenters identify several uncertainties on liability, including to the applicability of current statutory liability protections to "third party providers, such as the public key certificate authority operated by the WBA that is essential to OpenRoaming or the various third-party

[85] AT&T Comments, PS Docket No. 11-60, at 13-14 (rec. Jul. 16, 2018) (citing Norton Symantec Corporation, *The Risks of Public Wi-Fi*, https://us.norton.com/internetsecurity-privacy-risks-of-public-wi-fi.html).

[86] AT&T Comments, PS Docket No. 11-60, at 14 (rec. Jul. 16, 2018).

[87] *See, e.g.*, NCTA Comments, PS Docket No. 20-285, at 14-15 (rec. Oct. 1, 2020). Congress granted immunity from liability to certain emergency communications providers. *See* Wireless Communications Act, Pub. L. No. 106-81, § 4, 113 Stat. 1286, (1999) (codified at 47 U.S.C. § 615a); New and Emerging Technologies 911 Improvement Act of 2008, Pub. L. 110–283, § 201(a), 122 Stat 2620 (amending 47 U.S.C. § 615a). In 2012, Congress also extended the liability protection under 47 U.S.C. § 615a to wireless carriers, public safety answering points, and users of wireless 9-1-1 service with respect to the release of subscriber information related to emergency calls or emergency services, the use or provision of 911, E911, or NG911 services, and other matters related to 911, E911, or NG911 services. *See* Next Generation 911 Advancement Act of 2012, Pub. L. No. 112-96, § 6506, 126 Stat. 156 (codified at 47 U.S.C. § 1472).

[88] NCTA Comments, PS Docket No. 20-285, at 15 (rec. Oct. 1, 2020). NCTA observes that Wi-Fi service providers also do not provide "subscriber" information to PSAPs to the extent they are able to provide any information at all about a non-subscriber member of the general public who accesses an open Wi-Fi access point to place a 911 call over Wi-Fi. NCTA Comments, PS Docket No. 20-285, at 15 (rec. Oct. 1, 2020). Consequently, NCTA states, providing Wi-Fi access point access for the purpose of enabling 911 communications may not fit within the protections offered by Section 615a(a), potentially opening Wi-Fi network operators up to significant risk if they specifically took measures to support emergency services. NCTA Comments, PS Docket No. 20-285, at 15 (rec. Oct. 1, 2020).

[89] NCTA Comments, PS Docket No. 20-285, at 16 (rec. Oct. 1, 2020) (concluding that that absent changes in liability protection at the federal and state levels to expressly cover Wi-Fi service providers, "Wi-Fi [access point] and network operators could be disproportionately exposed compared to other providers of 911 emergency services.").

[90] Joint Commenters Comments, PS Docket No. 20-285, at 12-15 (rec. Oct. 1, 2020) (urging the Commission to "recommend that Congress enact legislation to confirm that the federal limits on liability related to 911 service extend to enterprises offering emergency services over Wi-Fi access and to their vendors" and noting that the patchwork of state laws on 911 can deter new 911 services as providers "cannot assess its potential liability should it deploy a nationwide service including 911 calling").

roaming exchange services such as Air Pass or Orion."[91] WBA concurs with the Joint Comments on extending 911 liability protections into the Wi-Fi domain, urges the Commission to address these concerns with relevant Congressional committees, and suggests that updating liability protections "would incentivize industry to work harder and faster towards enabling emergency services over Wi-Fi as a backup to the primary mobile networks."[92]

41. *Alternative Means of 911 Access*. While facilitating 911 access over Wi-Fi in emergencies is an important option to be pursued, it should not be viewed to the exclusion of other alternatives, such as making mobile networks more resilient and reliable so they are less likely to be unavailable in emergencies. Following the 2017 Atlantic hurricane season, the Commission has taken several steps to re-examine the Wireless Resiliency Cooperative Framework for purposes of restoring communications during and following disasters, including seeking comment on wireless carrier coordination efforts with backhaul and power providers.[93] In addressing the response to the 2017 Atlantic Hurricane season, CTIA states that the flexibility afforded by the Framework "gave carriers the freedom to experiment with and develop new and innovative techniques to restore service in the aftermath of the 2017 hurricanes."[94] CTIA observes that "AT&T used a 'flying cell on wings,' or a drone cell site, to temporarily provide data, voice, and text services over a forty mile radius in Puerto Rico in the aftermath of Hurricane Maria."[95] Drone cell sites, cells on wheels (COWs), and other mobile cell sites could be used to provide access to 911 services when mobile service is unavailable. We note, however, that these examples are not alternatives to mobile networks but instead are mechanisms for keeping mobile networks operational.

42. Under a flexible and voluntary framework, CTIA observes that "wireless providers are investing billions of dollars in resilient infrastructure, collaborating among competitors, working across industries and with local governments, and deploying innovative solutions to respond to evolving emergencies."[96] In Puerto Rico, for example, most of the backhaul fiber was aerial fiber placed on electric utility poles, and Hurricanes Irma and Maria destroyed many poles, "knocking out both electric

---

[91] Joint Commenters Comments, PS Docket No. 20-285, at 17 (rec. Oct. 1, 2020). The Joint Commenters also ask "whether [existing federal] laws encompass enterprises that decide to offer emergency services and include 911 call forwarding as a capability of their Wi-Fi service;" whether enterprises offering Wi-Fi access or third-party roaming exchange services "qualify as an 'IP-enabled voice [i.e., interconnected VoIP] service provider' . . .;" and whether liability protection "extends to vendors that manufacture, sell, install, test and support Wi-Fi access points." Joint Commenters Comments, PS Docket No. 20-285, at 15-17 (rec. Oct. 1, 2020).

[92] WBA Reply, PS Docket No. 20-285, at 6 (rec. Oct. 16, 2020) (stating that "[l]iability protections for authentication service providers are vital to delivering an end-to-end 911 over Wi-Fi solution.").

[93] *See Public Safety and Homeland Security Bureau Seeks Comment on Improving Wireless Network Resiliency to Promote Coordination through Backhaul Providers*, PS Docket No. 11-60, Public Notice, 33 FCC Rcd 11742 (PSHSB 2018) (*Backhaul Public Notice*); *Public Safety and Homeland Security Bureau Seeks Comment on Improving Wireless Network Resiliency Through Encouraging Coordination with Power Companies*, PS Docket No. 11-60, Public Notice, 34 FCC Rcd 47 (PSHSB 2019) (*Power Public Notice*); Press Release, FCC, FCC Launches Re-Examination of Wireless Resiliency Framework in Light of Recent Hurricanes, Agency Sends Letters to Framework Signatories Asking Them to Provide Post-Disaster Action Reports (Nov. 6, 2018), https://docs.fcc.gov/public/attachments/DOC-354963A1.pdf; *see also* FCC, *FCC Seeks Industry Input in Review of Wireless Resiliency Framework* (Nov. 6, 2018), https://www.fcc.gov/document/fcc-seeks-industry-input-review-wireless-resiliency-framework for the individual letters sent to each of the signatories.

[94] CTIA Comments, PS Docket No. 17-344, at 12 (rec. Jan. 22, 2018); *see also* AT&T Reply, PS Docket No. 17-344, at 9 (rec. Feb. 21, 2018).

[95] CTIA Comments, PS Docket No. 17-344, at 12 (rec. Jan. 22, 2018); *see also* AT&T Reply, PS Docket No. 17-344, at 9-10 (rec. Feb. 21, 2018).

[96] CTIA Reply, PS Docket No. 20-285, at 5 (rec. filed Oct. 16, 2020).

and wireless service at once."[97] T-Mobile's recovery efforts thus focused primarily on alternative backhaul solutions, such as utilizing wired backhaul from other LECs and deploying new satellite and microwave links for wireless backhaul.[98] With better information from backhaul providers regarding the status of their restoration efforts and priorities, T-Mobile submits that it would be better equipped to target and optimize its backhaul restoration planning.[99] In addition, CTIA states that Verizon "deployed portable facilities that used satellite connectivity for backhaul purposes in some limited circumstances, so the provider was not dependent on landline connectivity."[100]

C. Costs and Public Safety Benefits

43. Based on the information available at this time, we cannot reasonably estimate the costs or benefits of making Wi-Fi access points and spectrum for unlicensed devices available for 911 services when mobile service is unavailable. As discussed above, the record indicates that there are significant technical and policy challenges to providing emergency 911 access over Wi-Fi access points and networks, which could be costly to address. In addition, while enhancing Wi-Fi access points to make 911 more reliable and accessible provides clear public benefits, requiring the provision of emergency 911 access over Wi-Fi access points and unlicensed spectrum may yield less benefit at greater cost than other alternatives, such as investing in making mobile networks that already support 911 more resilient and reliable – and therefore more likely to remain available in emergencies. Thus, as better cost/benefit data becomes available, it will be important to weigh the relative costs and benefits of the specific alternatives discussed in this report against other possible approaches.

[97] AT&T Comments, PS Docket No. 11-60, at 14 (rec. Jul. 16, 2018); T-Mobile Comments, PS Docket No. 11-60, at 9 (rec. Jul. 16, 2018).

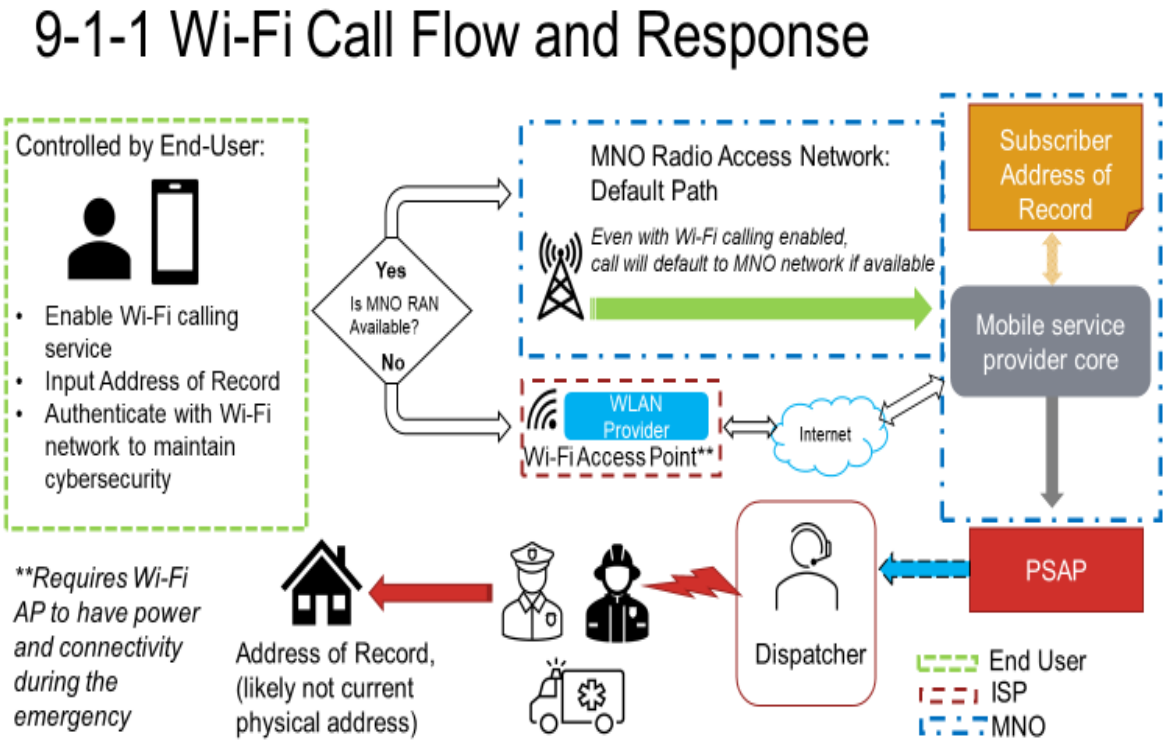
[98] T-Mobile Comments, PS Docket No. 11-60, at 9 (rec. Jul. 16, 2018).

[99] T-Mobile Comments, PS Docket No. 11-60, at 9 (rec. Jul. 16, 2018).

[100] CTIA Comments, PS Docket No. 17-344, at 13 (rec. Jan. 22, 2018).

APPENDIX A

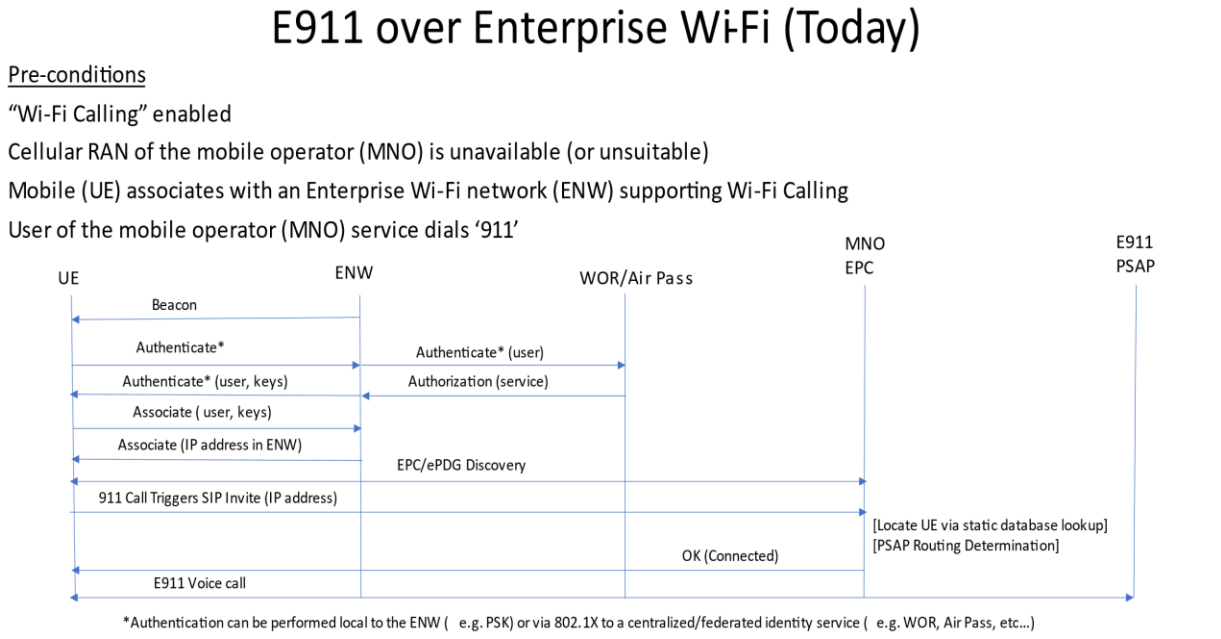
911 Wi-Fi Call Flow and Response[101]



[101] *See* NCTA Feb. 22, 2021 *Ex Parte* at Attachment.

APPENDIX B

911 Call Flow and Enterprise Wi-Fi[102]



[102] Joint Commenters Feb. 11, 2021 *Ex Parte* at Attachment (illustrating 911 call flow in the enterprise Wi-Fi context and enhanced 911 using Open Roaming/Air Pass platforms).

E911 over Enterprise Wi-Fi (Possible Enhancements)

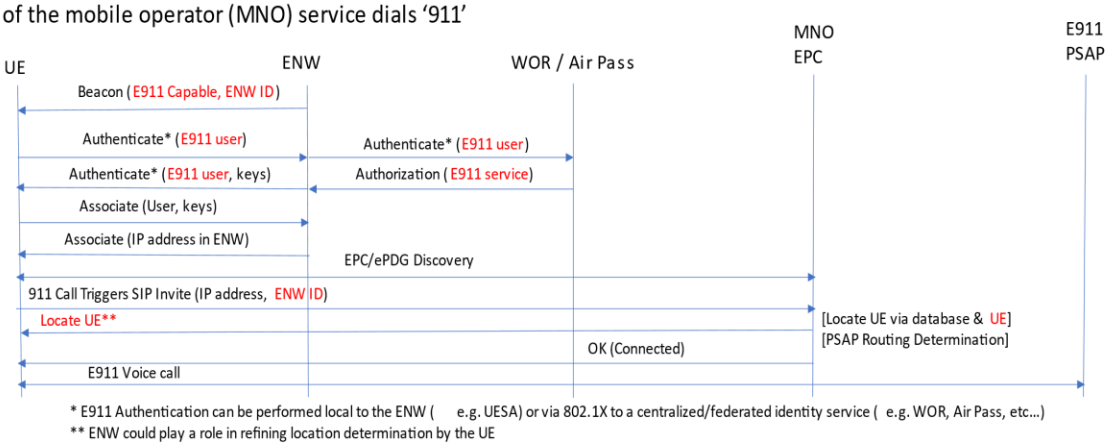
Pre-conditions

"Wi-Fi Calling" enabled

Cellular RAN of the mobile operator (MNO) is unavailable (or unsuitable)

Mobile (UE) is within acceptable coverage of an E911 capable Enterprise Wi-Fi network (ENW)

User of the mobile operator (MNO) service dials '911'



* E911 Authentication can be performed local to the ENW (e.g. UESA) or via 802.1X to a centralized/federated identity service (e.g. WOR, Air Pass, etc...)

** ENW could play a role in refining location determination by the UE

Post-conditions

E911 Call carried over Enterprise Wi-Fi network with enhanced QoS and privacy

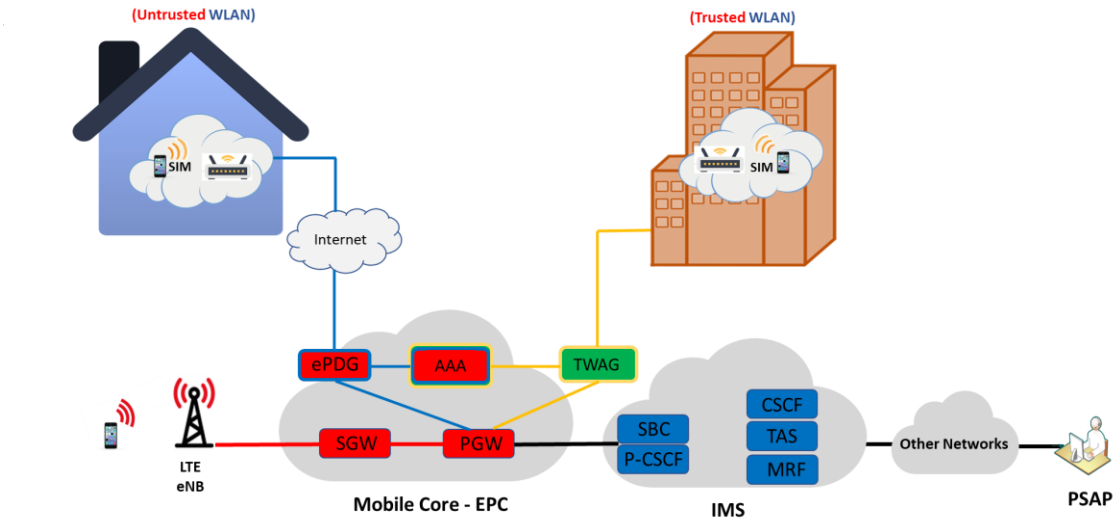
See: 3GPP TS 23.167

Glossary

- UE – user equipment such as a smartphone or laptop, also known as client device
- ENW – enterprise Wi-Fi network
- WOR/Air Pass: Wireless Broadband Alliance Open Roaming/Air Pass are two brands of open authentication platforms developed to allow WiFi clients to roam seamlessly and securely on networks that choose to host the roaming capability
- EPC – evolved packet core of mobile network operator networks; the EPC is generally composed of four network elements: the Serving Gateway, the Packet Data Network Gateway, the Mobility Management Entity (control plane) and the Home Subscriber Server.
  - ePDG discovery: EPC Packet Data Network Gateway
- Authentication – the UE establishes its identity with the network access point
  - "Keys" refers to encryption keys – see PSK below
- Association – the UE gains the ability to utilize the WiFi network under the terms it has been granted access (full, guest (Internetonly), or possibly in the future– emergency 911)
- PSK – pre-shared key; string of digits or password used to generate encryption keys for a client device or UE to permit secure communications
- QoS – quality of service

APPENDIX C

Mobile Core Network Access and Authentication



eNB	Evolved Node B (Base Station)
SIM	Subscriber Identity Module
SGW	Serving Gateway
PGW	PDN (Packet Data Network) Gateway
EPC	Enhance Mobile Core
ePDG	evolved Packet Data Gateway
TWAG	Trusted WLAN (Wi-Fi) Access Gateway
AAA	Authentication, Authorization and Accounting (server)
SBC	Session Border Control
IMS	IP Multimedia Subsystem (Deployed to facilitate deployment of various service, including VoLTE)
CSCF	Call Session Control Function
P-CSCF	Proxy CSCF
TAS	Telephony Application Server
MRF	Media Resource Function
PSAP	Public Safety Answering Point
WLAN	Wireless Local Area Network